A Model for Privacy in Public-Private Sector RFID Systems

Type of Submission: Full Research

Marta Vos
Whitireia New Zealand
Faculty of Business and IT
DX Box: SX33459
New Zealand
Email: marta.vos@whitireia.ac.nz

Rowena Cullen
Jocelyn Cranefield
School of Information Management
Victoria University of Wellington
Wellington, New Zealand
Email: Rowena.cullen@vuw.ac.nz; Jocelyn.cranefield@vuw.ac.nz

Abstract

This research identifies a model of factors affecting privacy in RFID systems that are shared between public and private sector organisations. Actor-Network Theory (ANT) is used as a framework for this research which identifies the nature of the data collected, voluntariness, legislation and security as factors affecting privacy, particularly within the public sector. In the private sector the desire for self-regulation and competitive advantage are seen. Across both sectors, understanding of the data collected by RFID systems, tailored staff access to data, and an unclear definition of privacy are identified. If these factors can be addressed, it is suggested that improved privacy, greater data sharing, and better understanding of the value of RFID data are possible outcomes.

Keywords

Privacy, RFID, ANT, Public Sector, Private Sector

INTRODUCTION

Privacy is a much debated issue in respect of today's technology systems yet despite the attention paid to the topic debate continues with research and publications continuing to focus on this issue. Smith, Dinev and Xu (2011) believe that privacy is context dependent however, many individuals and organisations struggle with understanding how *privacy* changes given the context in which they operate. A common source of confusion arises from the separation of privacy of the individual from confidentiality of business data – with the two definitions often being muddled. This observation has led Bélanger and Crossler (2011) to call for the examination of privacy to expand beyond the individual level and include organisational viewpoints and contexts. This confusion is particularly evident in a number of modern technological systems, especially those generating large distributed data sets such as those generated by Radio Frequency Identification (RFID) systems.

Privacy is a frequently cited issue in the implementation of Radio Frequency RFID systems (for example Ting et al. 2011, Yao et al. 2011, Zhou and Piramuthu 2010), with the majority of these studies being focused on private sector RFID implementations. RFID systems are seen to create privacy risks as they gather large amounts of data from tags placed on individually identifiable items. These large data sets can contain information from the very basic identification of the location of a particular item based on static readers and passive RFID tags; to the complex, identifying the movement of an item using GPS. The most complex tags can even report the physical condition of an item (Glover and Bhatt, 2006). RFID tags can also be used to identify the owner of a particular item (if they are carrying that item), and possibly to track that person (United Nations 2006).

Despite the frequent citing of privacy as a barrier to RFID implementation and adoption, in a review of 666 academic publications Irani, Gunasekaran and Dwivedi (2010) found that only 8% of publications in respect of RFID dealt with adoption, and only 7.5% discussed the legal, political, social or economic aspects of RFID technology. Research is also lagging in the area of government, and e-government RFID systems according to Mukerji and Palanisamy (2011) and Smith et al. (2011). Further, while there is some research on RFID systems

that are shared between public and private sector organisations, this research is primarily in the healthcare and defence areas where RFID technology is more widely used (Banks et al. 2007).

Thus, there is a gap in research considering privacy at an organisational level, particularly where RFID systems are shared between public and private sector organisations. This research focuses on this gap in the literature, attempting to determine the factors that affect privacy at an organisational level in public/private RFID systems. A qualitative approach is adopted as this research focused on a complex real life issue about which there is little known, and the researchers did not seek to influence proceedings (Creswell, 2009; Yin, 2009).

Privacy in RFID Systems – Prior Research

RFID systems are based on items bearing RFID tags, each tag carrying a unique identification (ID) numbers These tags can be read by RFID readers, which then send the read ID number to a central database which records the ID number of the tag, along with the time of the read, and the location of the reader. Simple passive RFID tags are generally only capable of transmitting their identifying details. More complex active RFID tags carry batteries and are capable of transmitting more information, for example temperature or environmental information. RFID tags can be very small, or almost invisible, and are common in identification cards, and retail items; tags can even be injected into humans or animals (Glover & Bhatt, 2006). According to Osyk, et al. (2012) RFID tags are becoming ubiquitous in today's environment, rapidly replacing barcodes in supply chain and warehousing applications.

The increasing ubiquity, and the near invisible nature of many RFID tags has given rise to concerns around the privacy of individuals carrying such tags. The reason for this concern comes from the nature of the RFID tags themselves. Firstly, the near invisible nature of many RFID tags means that individuals may not know they are carrying tagged items. Secondly, the majority of RFID tags are passive and have no security, or ability to be secured, they simply respond to any RFID reader within range. Thus passive RFID tags are always on, and able to be tracked by anyone with the capability to read and decode the tag (United Nations, 2006). This could allow for the unauthorised reading of RFID tags being carried by individuals, either to identify the items being carried, or to track the individuals themselves (Krotov & Junglas, 2008)."

Yao, Chu and Li (2011) in a study of RFID adoption literature found privacy was a primary barrier to adoption, along with technical difficulties and cost. Wamba (2012) examined RFID implementation in healthcare and found that in 22 articles the majority cited privacy, security and data management as barrier to implementation. In a study specifically directed at public sector use of RFID, Neuby and Rudin (2008) found barriers included privacy and cost. In e-government, Mukerji and Palanisamy (2011) found barriers to adoption included legal and cost issues. The European Union (European Commission, 2013; European Union, 2009) has been active in producing guidelines in relation to how EU governments should handle RFID systems specifically, identifying policy development and data management as areas that should be paid particular attention.

RFID systems also generate immense databases, which are stored for possibly unlimited periods of time. Michelfelder (2010) argues that these features infringe the rights of individuals to decide how and when they relate to information technology, as information about them can be stored without their consent, or even knowledge. The European Commission (2013) stated that individuals should be able to opt out of having data collected from any RFID tags they carry, even if those tags are invisible. The European Commission (2006) also recognises a distinction between tags that identify individuals (or that could identify individuals), and those that identify goods or services. The Commission states that tags identifying items do not give rise to privacy concerns *per se*, whereas privacy problems can arise when individuals can be identified through RFID tags. King and Jessen (2010) list possible privacy issues as including the possible tracking of individuals, possible identify theft, and exposure to unsolicited advertising.

Miorandi et al. (2012), discuss this issue in relation to the business context, noting that business data is an asset also requiring protection against possible breach. They believe that business data can be considered confidential rather than private, defining confidentiality as "the guarantee that only authorised entities can access and modify data" (Miorandi et al., 2012, p. 1505). Like the European Commission (2013) they believe that privacy solutions are still a challenge in today's environment, despite the increasing number of technology solutions available. Although a number of solutions have arisen to the problem of unauthorised collection of data from RFID tags, such as tag deactivation (Ohkubo, Suzuki, and Kinoshita, 2005), or tag blocking (United Nations, 2006), these solutions still present challenges, primarily that RFID tags can be invisible, and individuals may not know they are carrying such tags.

THEORY AND METHODOLOGY

As RFID systems can be seen to be complex assemblages of social and technological elements, the nature of the technology being investigated indicated that a theoretical framework encompassing a mixture of human and non-

human technological actors would be most appropriate. Therefore Actor Network Theory (ANT), with its inclusion of technology within a model of the social was considered the most suitable framework within which to study privacy in public/private RFID systems. The symmetrical view adopted by ANT, where all human and non-human actors have agency, and are able to act, allowed cross sector RFID systems to be investigated in a more comprehensive way than might be possible with a theory that denied the agency of technology.

However, as noted by Gad and Jensen (2010), ANT has no specific methodology even though some methods align with ANT studies. As a result ANT does not dictate how a study must be conducted, just as it refuses to dictate how society must be formed. Thomas (2006), in a summary of ANT studies noted that authors reported taking a "general inductive approach" (p. 238) to data gathering and analysis, and recommends a sound qualitative methodology is indicated in the pursuit of ANT based research. Although there is little explicit methodology offered by ANT, there is one point on which ANT researchers agree, the advice of Latour (2002) and Callon (1991) to "follow the actors", as the actors (human or non-human), and their associations for the basis of an ANT description. As explained by Latour (1999), ANT is not so much a theory as a way to allow the actors within a particular network to have a voice. He recommends using the simplest of language to give voice to the actors, wherever possible using their own words - as has been done in the findings section, where the voices of the actors are used in quotation marks as part of the description (Latour, 2005). Similarly Cresswell, Worth and Sheikh (2010) consider ANT to be a way of describing how the connections occur between actors, as well as a way to locate parts of the network through following the actors.

This research focused on RFID systems that were shared between the public and private sectors, thus the actors interviewed had to have knowledge of such systems. In total 40 human actors were interviewed, over a period from 2011 to 2012. The in-depth interviews lasted between one and two hours, and were digitally recorded and transcribed. Following the advice of Latour and others, no questions were pre-supposed, rather the interviewer allowed the interview to proceed in the direction in which the interviewees wanted to take it. The interviewees received a copy of the interview transcript, and were able to correct and respond to these. All interviewees had at least two years' experience with cross sector RFID systems, and could speak on behalf of their own actions, or on behalf of their organisations. Actors were located by asking interviewees for recommendations to others, through a process of snowballing (Yin, 2009). Alternatively, actors were located through the need to find representatives for non-human actants within the RFID network, following the suggestion of Vidgen and McMaster (1996). This demonstrated the strength of the ANT approach, as it was possible to locate actors to speak on behalf of the RFID technology, as an expert in RFID tags could speak for this part of the network, or an expert on RFID implementation could represent the RFID system itself. Further, 24 documentary actors in the form of business cases, legislation, reports and standards, were also included in the coding, and in the final analysis. The inclusion of these non human actors, and the representatives of some of the technology components, allowed for a much richer picture to be built of RFID technology in the public-private context. The study ceased looking for new actors when no new actors were recommended – in other words when the point referred to by Corbin and Strauss (2008) as saturation was reached. This is similar to Bonner and Chiasson (2005), in their research on privacy legislation, where they followed actors through documents, publications and interviews until no new information was found.

The data was analysed using the "general inductive approach" recommended by Thomas (2006, p. 238). The purpose of the analysis was to allow findings to emerge from the interview data, without constraining the findings with a strict methodology. Therefore, this style of analysis suits the ANT approach with its lack of specific analysis method. Data was coded through a series of cycles, the first being mostly inductive, using the words of the actants to form the codes themselves. Some deductive codes were also used in this first cycle primarily to identify elements of the RFID systems, the nature of the system being discussed (public or private, supply chain, sensor or other types of RFID applications), and the ontology of ANT. The second cycle consisted of pattern coding, followed Miles, Huberman and Saldana (2013). This cycle identified connections between the actors, and to help explain the data. The first cycle codes were grouped into summary categories. This allowed for the identification of higher level issues, and mediators that related to the way RFID systems were constructed and operated. During this process categories were assigned to raw data, through an inductive process involving detailed, considered and repeated reading of the text. Parts of coded transcript were checked by each of the authors, and discussed, in order to ensure consistency and rigour. Categories were also discussed, detailed by memos, and revised if necessary.

These categories formed the basis of the model presented in the findings. Each higher level category was seen to play a role in the interaction between RFID systems and the environment, particularly in relation to how the issue of privacy influences such systems.

FINDINGS

Privacy considerations were apparent across many different aspects of cross sector RFID systems, from discussions of the privacy of individuals using RFID systems, to data and organisational privacy (or confidentiality). Emphasis was placed on understanding the purpose of data collected by RFID systems, and ensuring that data was appropriately used.

The sector of the organisation played a role in the approach the organisation took to privacy. Public sector organisations were seen to be more concerned with privacy issues, whereas the private sector found privacy to be "not so much of an issue". This finding was related in part to the nature of the information collected by public sector organisations, with one actor believing that "governments need to more carefully understand privacy implications than private sector companies that sell to other businesses (as opposed to consumers)." Further, the lack of choice (or voluntariness), in provision of data to the public sector was seen to increase sensitivity to privacy. As one actor stated "if [the government] muck up how they handle your information, you've still got to keep handing them information...". Where involvement in an RFID system was mandated by law, public sector organisations were seen to be careful to ensure that the data collected was defined by an enabling act where "under the [enabling] legislation it is very clear in the purposes of the Act what exactly information collected can be used for, and it is very narrow." In a number of mandated implementations "there is an entire section within [the act] around rights of access to information and it quite clearly separates the personal from the impersonal, non-personal".

The private sector had a different view of privacy being legislated, preferring to self-regulate. One actor had been involved in a cross sector implementation where it was considered that it was important to ensure that "governments don't step in and legislate or mandate [privacy] things that are not necessarily in the best interests...". Private sector actors felt that data sharing agreements should be sufficient to "get around the privacy concerns and everything else around the use of data because [organisations] should be in arrangements with their suppliers that [sharing of data] is okay to happen". Even though all the countries studied had a form of privacy legislation in place, it was apparent that uncertainty existed around how to handle personal data within RFID systems.

Organisations in both sectors were reluctant to share data, although for different reasons. Private sector organisations cited concerns around "competitive advantage" for not wanting to share data. In contrast public sector organisations were concerned about systems privacy (as above) and security, with one actor involved in an implementation where data would have to be transmitted from a secure to a non-secure system and the public sector organisation involved "didn't want the two touching". Another actor commented that he could not "think of any times where [public sector organisations] feedback data to a commercial system".

A number of the RFID implementations studied crossed international borders, and difficulties became apparent in understanding how to handle personal information across jurisdictions. One actor commenting that because of the lack of a "common international view [on privacy], in the end most conversations around trade facilitation actually pivot on privacy as opposed to being facilitated by meeting privacy requirements". This actor saw an answer to privacy issues as allowing for "the data and price questions [to] become more easily answered, because it's much easier to talk about what the real value of the data is internationally when you overcome the issue of how we manage privacy".

The solution to the problem of understanding privacy in RFID systems was seen to arise from having "a clear understanding of the purpose for which the information was collected". This understanding turned on the difference between data that could be connected to individuals compared to data that related to *things*. For example one actor pointed out that "mangoes have no privacy, they are a vegetable or fruit... why would their privacy be infringed?" The design of such solutions appeared to relate to the abilities of the RFID technology, "what the technology can do, what it can't do, what it is designed to do, what it is designed not to do". However, a problem with organisational understanding of RFID systems was highlighted by one actor who found that "for most of [my customers] they don't really know what's going to happen and they don't really know the implications of what they are doing". He had found that discussions around implementation of RFID systems "usually end up in discussions about how [the data] is being used, [and] about any privacy aspects for what they're doing, if that is even applicable". Another actor highlighted the need to ensure data is accessed only by those authorised to access it, as he commented "if you have a database of all your customers you want to have that database only accessible by the people that need to access it for their jobs, you don't want it to be completely open so that anyone in the [organisation] can dip in and out".

DISCUSSION

These qualitative findings suggest a model of factors affecting privacy in public/private RFID systems, summarised in Table 1. The public sector was seen to be more sensitive to privacy because of a combination of

the nature of the data collected, and the lack of perceived voluntariness in the provision of that data. Legislation also framed how the public sector used RFID generated data, and the need to secure public sector systems affected how the public sector interacted with private sector partners.

Table 1: Privacy Factors in RFID Implementations

Public Sector	Private Sector
Nature of Data	Self-Regulation
Voluntariness	Competitive Advantage
Legislation	
Security	
Both Sectors	
Understanding of Data Collected	
Staff Access	
Unclear Definition of Privacy	
Outcomes	
Improved Privacy	
Data Sharing	

The private sector was seen to be conscious of competitive advantage, and reluctant to share data because of this. Private sector organisations were also keen to self-regulate rather than having legislation dictate the terms of their involvement with public sector organisations.

Both sectors were affected by a lack of understanding of the data collected by RFID systems, with a sound understanding of the type of data collected being seen to improve both the privacy of the data, and the sharing of that data. Better understanding of data collected by RFID systems was also seen to improve the ability of organisations to tailor access of staff to databases containing such information. The lack of a clear definition of privacy at an international level was seen to affect discussions in relation to cross border RFID applications, in that it led to difficulties determining how data was to be shared, secured, and valued. A clearer definition was seen as a way to provide improved outcomes in this area. The finding that the definition of privacy is unclear is not a new one. Smith et al. (2011) also noted this in their summary of privacy literature. However, the importance of a common definition at an international level has seldom been demonstrated.

It is worth noting that the data used in this study was collected from RFID applications that were shared by public and private partners, therefore, it can be seen that within the same context (of public/private RFID systems) public sector organisations were more sensitive to the nature of the data collected, the method used to collect it (voluntariness), to the legislation applying to that data, and to the need to secure it. This finding alerts private sector organisations to the need to consider privacy requirements in applications shared with public sector partners. Further it warns public sector organisations that private sector partners may not be as conscious of privacy requirements in such shared systems.

Overall this study demonstrates the need for organisations to clearly understand the nature of the data they collect from RFID systems, and to understand the drivers of privacy in cross sector organisational partners. In public/private RFID systems the different concerns organisational partners have in relation to privacy can inhibit data sharing, and a even understanding the value of data collected by the RFID systems.

The use of ANT in this study has been particularly illuminating. The ability to follow actors both human and non-human through the various public/private RFID applications studied, allowed for a rich picture of these RFID based systems to be developed. The view of privacy described here was just a small part of the complexity that emerged, and highlights the utility of using ANT as a basis to describe the factors affecting complex technology systems.

LIMITATIONS

The qualitative nature of this study limits the ability to generalise from it, a limitation common to qualitative interpretivist research. However, sound methodology and research design, with attention paid to reliability in coding, allows for trustworthiness in the results (Richards and Morse 2007). Similarly, it was not possible to interview all actors present within particular RFID systems studied because of time and distance constraints.

CONTRIBUTION AND FUTURE RESEARCH

This study contributes to research by addressing the call of Smith et al. (2011) to further understand privacy in the organisational context. It also addresses a gap in research regarding how privacy works in RFID systems that are shared between public and private sector organisations.

This study also contributes to practice by highlighting the disparity in the way privacy is viewed in public/private RFID systems. This alerts organisational partners to possible difficulties in the way privacy may be viewed across sectoral boundaries and emphasises the need to ensure all parties agree on a common view of privacy. A greater understanding of the nature of the data collected, along with this common view, will likely improve the privacy of RFID generated data in the public/private context.

Further, the use of ANT suggests a method by which complex technological networks, such as those related to cloud computing or big data, can be understood. This is not only from the point of view of privacy, but in relation to the factors that influence technology network creation and development. The use of ANT in this research allowed for the development of a model of privacy that can be further investigated quantitatively, both from the perspective of testing the factors found to affect privacy, and from the perspective of other similar technological networks.

This research was aimed at increasing our understanding of a phenomenon that is still emerging. Thus a qualitative approach was taken, according to Yin, 2009. However, the model that was developed can be used as the basis for a quantitative examination of attitudes towards and perceptions of privacy in public/private RFID systems.

REFERENCES

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems". *MIS Quarterly*, (*35*:4), pp 1017–1042.

Bonner, W., and Chiasson, M. 2005. "If Fair Information Principles are the Answer, What was the Question? An Actor-Network Theory Investigation of the Modern Constitution of Privacy". *Information and Organization*, (*15*:4), pp 267–293. doi:10.1016/j.infoandorg.2005.03.001

Callon, M. 1991. "Techno-economic Networks and Irreversibility". *A Sociology of Monsters: Essays on Power, Technology and Domination*, *38*, pp 132–161.

Corbin, J. M., and Strauss, A. L. 2008. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Los Angeles, Calif.: Sage Publications.

Cresswell, K. M., Worth, A., and Sheikh, A. 2010. "Actor-Network Theory and its Role in Understanding the Implementation of Information Technology Developments in Healthcare". *BMC Medical Informatics and Decision Making*, (*10*:1), pp 67. doi:10.1186/1472-6947-10-67

Creswell, J. 2009. *Research Design: Qualitative, Quantitative, and Mixed Method Approaches* (3th ed.). Thousand Oaks: Sage Publications.

European Commission. 2013. *Report on the Public Consultation on IoT Governance*. European Commission. Retrieved from https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

European Union. 2009. *Internet of Things - an Action Plan for Europe* (No. 278). Brussels: Commission of the European Communities. Retrieved from http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

Gad, C., and Jensen, C. B. 2010. "On the Consequences of Post-ANT". *Science, Technology & Human Values*, (*35*:1), pp 55 –80. doi:10.1177/0162243908329567

Glover, B., and Bhatt, H. 2006. *RFID Essentials*. Sebastopol CA: O'Reilly.

Irani, Z., Gunasekaran, A., and Dwivedi, Y. K. 2010. "Radio Frequency Identification (RFID): Research Trends and Framework". *International Journal of Production Research*, (*48*:9), 2485. doi:10.1080/00207540903564900

King, N. J., and Jessen, P. W. 2010. "Profiling the Mobile Customer - is Industry Self-regulation Adequate to Protect Consumer Privacy when Behavioural Advertisers Target Mobile Phones? - Part II". *Computer Law & Security Review*, (*26*:6), pp 595–612. doi:10.1016/j.clsr.2010.09.007

Krotov, V., and Junglas, I. 2008. "RFID as a Disruptive Innovation". *Journal of Theoretical and Applied Electronic Commerce Research*, (*3*:2), 44.

Latour, B. 1999. *Science in Action: How to Follow Scientists and Engineers Through Society*. Cambridge Mass.: Harvard University Press.

Latour, B. 2002. *Aramis, or, the Love of Technology* (4th ed.). Cambridge Mass.: Harvard University Press.

Latour, B. 2005. *Reassembling the Social: An Introduction to Actor-Network Theory*. Oxford; New York: Oxford University Press.

Michelfelder, D. P. 2010. "Philosophy, Privacy, and Pervasive Computing". *AI & Society: Knowledge, Culture and Communication*, (*25*:1), pp 61–70. doi:10.1007/s00146-009-0233-2

Miles, M. B., Huberman, A. M., and Saldana, J. 2013. *Qualitative Data Analysis: An Expanded Sourcebook* (3rd ed.). Thousand Oaks: Sage Publications.

Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. 2012. "Internet of Things: Vision, Applications and Research Challenges". *Ad Hoc Networks*, (*10*:7), pp 1497–1516. doi:10.1016/j.adhoc.2012.02.016.

Mukerji, B., and Palanisamy, R. 2011. "The RFID Technology Adoption in e-Government: Issues and Challenges". *International Journal of Electronic Government Research*, (*7*:1), pp 89–101. doi:10.4018/jegr.2011010106.

Neuby, B. L., and Rudin, E. 2008. "Radio Frequency Identification: A Panacea for Governments?" *Public Organization Review*, (*8*:4), pp 329–345.

Ohkubo, M., Suzuki, K., and Kinoshita, S. 2005. "RFID Privacy Issues and Technical Challenges". *Communications of the ACM*, (*48*:9), pp 66. doi:10.1145/1081992.1082022.

Osyk, B.A., Vijayaraman, B. S., Srinivasan, M., and Dey, A. 2012. "RFID Adoption and Implementation in Warehousing". *Management Research Review, (*35:10), pp 904-926.

Richards, L., and Morse, J. M. 2007. *Readme First for a User's Guide to Qualitative Methods* (2nd ed.). Thousand Oaks Calif.: Sage Publications.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review". *MIS Quarterly*, (*35*:4), pp 989–1016.

Thomas, D. R. 2006. "A General Inductive Approach for Analyzing Qualitative Evaluation Data". *American Journal of Evaluation*, (*27*:2), pp 237 –246. doi:10.1177/1098214005283748.

Ting, S. L., Kwok, S. K., Tsang, A. H. C., and Lee, W. B. 2011. "Critical Elements and Lessons Learnt From the Implementation of an RFID-Enabled Healthcare Management System in a Medical Organization". *Journal of Medical Systems*, (*35*:4), pp 657–669. doi:10.1007/s10916-009-9403-5.

United Nations. 2006. *Legal Issues of RFID Technology*. United Nations. Retrieved from http://www.rfidconsultation.eu/docs/ficheiros/Legal_issues_of_RFID_technology_LEGAL_IST.pdf.

Vidgen, R., and McMaster, T. 1996. "Black Boxes, Non-Human Stakeholders and the Translation of IT Through Mediation". In W. Orlikowski, G. Walsham, M. R. Jones, & J. I. DeGross (Eds.), *Information Technology and Changes in Organizational Work: Proceedings of the IFIP WG8.2 Working Conference on Information Technology and Changes in Organizational Work, December 1995* pp. 250–271. London: Chapman & Hall on behalf of the International Federation for Information Processing (IFIP).

Wamba, S. F. 2012. "RFID-Enabled Healthcare Applications, Issues and Benefits: An Archival Analysis (1997-2011)". *Journal of Medical Systems*, (*36*:6), pp 3393–8. doi:http://dx.doi.org.helicon.vuw.ac.nz/10.1007/s10916-011-9807-x.

Yao, W., Chu, C. H., and Li, Z. 2011. "The Adoption and Implementation of RFID Technologies in Healthcare: A Literature Review". *Journal of Medical Systems*. (36:6) pp3507-3525.

Yin, R. 2009. *Case Study Research: Design and Methods* (4th ed.). Los Angeles Calif.: Sage Publications.

Zhou, W., and Piramuthu, S. 2010. "Framework, Strategy and Evaluation Health Care Processes with RFID". *Decision Support Systems*, (*50*:1), pp 222–233. doi:10.1016/j.dss.2010.08.003.

ACKNOWLEDGEMENTS

This research was supported by the EPCglobal/GS1 New Zealand Scholarship. The authors would like to thank EPCglobal New Zealand for their support.

COPYRIGHT